2012 International Conference on System Science and Engineering
June 30-July 2, 2012, Dalian, China

A New Chaotic System for Image Encryption

Long Bao[a], Yicong Zhou[b,*], Member, IEEE, C. L. Philip Chen[b], Fellow, IEEE, Hongli Liu[a]
[a] College of Electrical and Information Engineering, Hunan University, Changsha, China
[b] Department of Computer and Information Science, University of Macau, Macau, China
[*] yicongzhou@umac.mo

Abstract—**With the increasing demand of providing security for images/videos with private information, chaos-based crypto-systems have played an important role in image encryption because of their excellent random properties and encryption performance. However, existing chaos-based systems have the security defect due to small key space or other security weakness. This paper introduces a new chaotic system using a combination of three conventional chaotic maps. The proposed chaotic system shows excellent chaotic behaviors. To demonstrate its application in image processing, a new image encryption scheme using the proposed chaotic system is also introduced. Computer simulation and security analysis demonstrate that the proposed image encryption scheme shows excellent encryption performance, high sensitivity to the security keys, and a sufficiently large key space to resist the brute attack.**

Keywords- image encryption; chaotic system

I. INTRODUCTION

Nowadays, information always plays a vital role in social communication. To deliver information, people utilize images, sounds, texts and videos to express what they want the others to know. Among these ways, the image is so popular for its authenticity and intuitiveness. With wide use of the images, especially the ones transmitting on the Internet, security of the images has become an imperative problem to deal with. Image encryption is an effective method to protect images by transforming them into an unrecognized format. In existing methods of image encryption, the chaos-based image encryption algorithms have many advantages for the random properties of chaotic maps/systems, such as sensitivity to initial values/system parameters and state ergodicity [1].

For these prominent features, the one/two/three-dimensional chaotic maps have been explored and utilized in the design of the image encryption algorithms since Matthews [2]. One-dimensional chaotic maps, like the Logistic map [3], Tent map [4], Sine map and Guass map [5], have been used in practice for their simple structures, fast encryption speed and limited calculation amount. In 1995, Phatak and Rao used the Logistic map to generate pseudorandom numbers [6]. In 2001, Sobhy and Shehata found that the opponent could identify a chaotic system with single one-dimensional chaotic map by using the iteration and auto-correlation function [7]. Then in 2006, a chaotic system employing two chaotic Logistic maps, to overcome the small space and other security issues, was applied to image encryption [8]. Although the chaotic system is simple, the encryption system is extremely complicated. In 2011, the chaos-based encryption systems have been well developed. However, in [9, 10], the authors intended to build a complicated encryption structure without considering the chaotic map itself to provide a high security level.

This paper introduces a new chaotic system which is composed of three different one-dimensional chaotic maps. The proposed system uses the Logistic map as a controller to choose the Tent map or Sine map to generate random sequences. The new system shows more complicated chaotic behaviors.

To simplify the structure of the encryption system while providing the high level of security, a new image encryption algorithm is then introduced using the proposed encryption system. To satisfy the Shannon's confusion and diffusion properties, the proposed encryption system uses the substitution-permutation network (SPN) structure [11]. To enhance the security level, the encryption and decryption keys with the size of 240 bits are known to be long enough to withstand the brute-force attacks. Computer simulation and security analysis will be given.

The paper is divided into five parts. In Section II, the new chaotic system will be introduced and its chaotic property will be also observed. Then in Section III, the SPN based encryption system using the new chaotic system will be proposed. Computer simulation and security analysis will be shown in Section IV. In Section V, a conclusion will be reached.

II. THE NEW CHAOTIC SYSTEM

This section introduces a new framework of the chaotic system.

The chaotic system consists of a control sequence generator and a chaotic sequence generator. The Logistic map is used for the control sequence generator to choose one of two maps: the Tent map and Sine map. In the part of the chaotic sequence generator, the Tent map and the Sine map are used as generating maps to generate the output chaotic sequence. The function F in Eqn. (1) represents the chaotic system. We use the control sequence to choose one of the generating maps.

$$X_{i+1} = F(X_i, q_i) = \begin{cases} f_1(X_i) & q_i = 0 \\ f_2(X_i) & q_i = 1 \end{cases} \quad (1)$$

$$f_1(X_i) = T(X_i) = \begin{cases} u * X_i & X_i < 0.5 \\ u * (1 - X_i) & X_i \geq 0.5 \end{cases} \quad (2)$$

$$f_2(X_i) = S(X_i) = a * \sin(\pi X_i) \quad (3)$$

Here, q_i is the i^{th} element of the control sequence produced by the Logistic map.

$$f_3(Y_i) = L(Y_i) = r * Y_i * (1 - Y_i) \quad (4)$$

978-1-4673-0945-5/12/$31.00 ©2012 IEEE

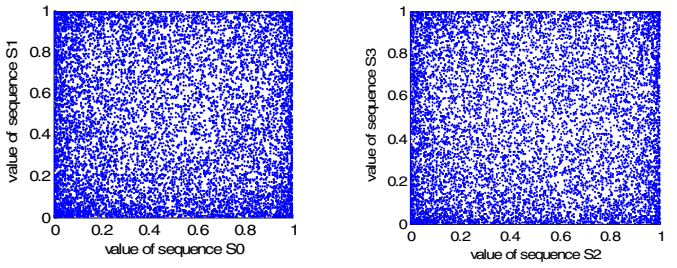
$$q_i = \begin{cases} 1 & f_3(Y_i) < 0.5 \\ 0 & f_3(Y_i) \geq 0.5 \end{cases} \quad (5)$$

To test the property of the new chaotic system, the simulation and analysis have been done. For a chaotic system, the sensitivity to the initial condition, including the initial value and parameters, is extremely important. This ensures that a slight alteration to the initial condition will result in a completely different result. This property also makes sure that an attacker cannot try to use an approximate value to rebuild the same system producing the same result.

Hence, a test with different parameters and the same initial value is designed to evaluate the system's sensitivity to parameters. Chaotic sequence S0 is generated by the proposed chaotic system with the parameter of the Logistic map equal to 3.999999. Sequence S1 is generated using 4 as the parameter of the Logistic map. The results are shown in Figure 1(a), where X axis indicates the value of the chaotic sequence S0 and Y axis is the value of the chaotic sequence S1. Moreover, to test the sensitivity to the initial values, we also apply the same parameter and different initial values to the new chaotic system. Chaotic sequence S2 is generated using the initial value as 0.099999. Sequence S3 is generated by the chaotic system in which the initial value is 0.1 as shown in Figure 1(b).

From Figure 1(a), it is easy to found that there is a huge difference between sequence S0 and sequence S1.This is because there is a little correlation between sequence S0 and sequence S1. The same result is obtained in Figure 1(b). These results confirm this new chaotic system shows a high sensitivity to both the initial values and the parameters.

To evaluate the chaotic system, the chaotic property with different parameters is observed to check its chaotic range. This new chaotic system contains three parameters in the Logistic map, Sine map and Tent map, respectively. To get the bifurcation diagram, a test with two parameters fixed is done as an example. The Figure 2 is generated by changing the parameter of the Sine map within [0, 1], while setting the parameter of the Tent map and Logistic map to 1.8 and 3.9, respectively. From the results in Figure 2, the chaotic range of the new chaotic system has been expanded. Altering all three parameters of the new system will result in better chaotic behaviors than conventional one-dimensional chaotic maps.



(a) (b)

Figure 1. Random-like relationship between two chaotic sequences generated by the new chaotic system under different conditions: (a) changing parameters; (b) changing initial values;

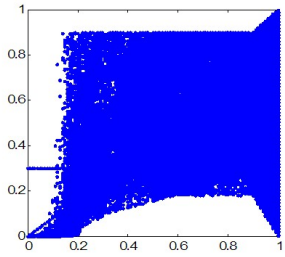


Figure 2. Bifurcation diagrams of the new chaotic system

III. THE NEW ENCRYPTION ALGORITHM

To apply the new chaotic system to the image encryption, this section introduces a new chaos-based image encryption algorithm. It is based on the structure of the substitution and permutation network (SPN). Figure 3 shows the image encryption procedure using a 6-round substitution and permutation. The image decryption is done by simply reversing the process.

This encryption algorithm contains three steps:

A. Get the parameter settings and initial values from the encryption key

In the new encryption algorithm, the encryption key with the length of 240 bits contains all the parameter settings and initial values of the new chaotic system. A different decrypted key will be generated by the encryption process with the same length of 240 bits.

$$Ke = K_0 K_1 K_2 K_3 K_4 K_5 K_6 K_7 K_8 K_9 \quad (6)$$

$$K_i = K_{i0} K_{i1} K_{i2} \cdots K_{i21} K_{i22} K_{i23} \quad (7)$$

The encryption key (denoted as Ke) is divided into 10 parts according to their functions which represent different parameters and initial values as shown in Table I.

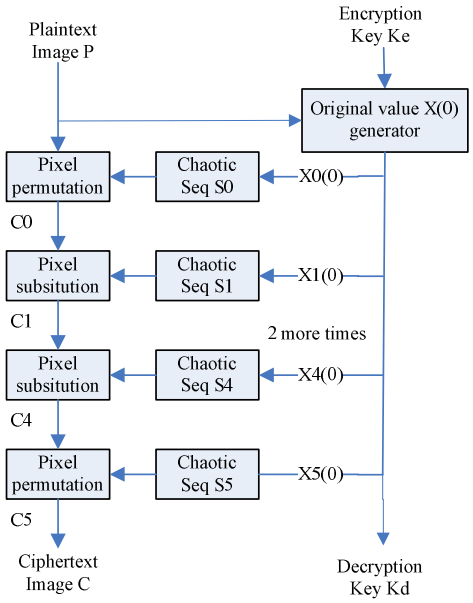


Figure 3. The proposed image encryption algorithm

TABLE I. FUNCTIONS OF TEN PARTS OF TEN ENCRYPTION KEY

Key part	Function
Ke0	To calculate the initial values of the Logistic map
Ke1	The parameter of the Logistic map
Ke2	The parameter of the Tent map
Ke3	The parameter of the Sine map
Ke4	The initial value of the S0 chaotic system
Ke5	The initial value of the S1 chaotic system
Ke6	The initial value of the S2 chaotic system
Ke7	The initial value of the S3 chaotic system
Ke8	The initial value of the S4 chaotic system
Ke9	The initial value of the S5 chaotic system

Here, K_i represents the i^{th} part of the encryption key with 24 bits. Ke_i stands for the decimal numbers calculated by Eqn.(8).

$$Ke_i = \frac{\sum_{j=0}^{23} K_{ij} \times 2^j}{2^{24}} \tag{8}$$

To improve the random properties of the new chaotic system, the parameters of three one-dimensional maps are set in the range where each one-dimensional map shows excellent chaotic behaviors. By the simulation of three one-dimensional maps, individually, it is easy to get the results. The range of the Logistic maps is between 3.8 and 4. The range of the Tent maps is between 1.5 and 2. The range of the Sine maps is between 0.9 and 1. So changes in the parameter settings are made according to Eqns. (9)-(11).

$$r = \frac{Ke_1}{5} + 3.8 \tag{9}$$

$$u = \frac{Ke_2}{2} + 1.5 \tag{10}$$

$$a = \frac{Ke_3}{10} + 0.9 \tag{11}$$

The decryption Kd is generated by the encryption system. The difference between Kd and Ke is the value of the first part (K_0) of the keys. Kd0 is defined in Eqn. (12).

$$Kd_0 = \frac{Ke_0 + K_p}{2} \tag{12}$$

Here, K_p is obtained from a given plaintext image P as shown in Eqn. (13). The value of F depends on the type of images to be encrypted. For the grayscale images, F is equal to 256.

$$K_p = \frac{\sum_{j=1}^{W}\sum_{i=1}^{L} P_{i,j}}{W * L * F} \tag{13}$$

Each initial value $X_i(0)$ (i=0, 1, 2, 3, 4, 5) of the Logistic map in the new chaotic system is decided by Kd_0 and the initial value Ke_i of the corresponding new chaotic system.

$$X_i(0) = \frac{Kd_0 + Ke_{i+4}}{2} \tag{14}$$

B. Generate the chaotic sequence

The new chaotic system generates the chaotic sequences at length of W×L. In the first step, the parameters of three one-dimensional maps and the initial values of the Logistic map are determined by the encryption key. Once the variables of the chaotic system are determined, the chaotic system is fixed and then starts to generate the chaotic sequences for image encryption.

C. Encrypt the input image

This paper uses the SPN structure to organize the framework of the image encryption process using the chaotic sequences. The SPN mainly consists of two basic operations: the pixel permutation and pixel substitution.

There are several different methods to perform the pixel permutation. This paper uses the chaotic sequence S with the length of W×L, produced by the proposed chaotic system, as reference matrix to scramble image pixel positions. The algorithm first changes the input image into one-dimension matrix column by column from left to right. Then by sorting the order of the sequence S, the chaotic sequence is changed into a sorted order. In relation of changing the sequence S, the same change is made to the one-dimensional image matrix to scramble pixels positions in the input image. By this way, the positions of pixels are upset and the image is unrecognized.

Although the pixel permutation will make the content of image unrecognized, the attacker will get some information by the histogram analysis to rebuild the image. Therefore, doing only the pixel permutation is not enough. Therefore, the pixel substitution is adapted to change the image histogram.

The random-like sequence S is used to encrypt the input image by using Eqn. (15).

$$C = \mathrm{mod}\ (floor(S * F) + P, F) \tag{15}$$

Here, the FLOOR(X) rounds the elements of X to the nearest integers towards minus infinity and MOD(x, y) is reminder of x/y.

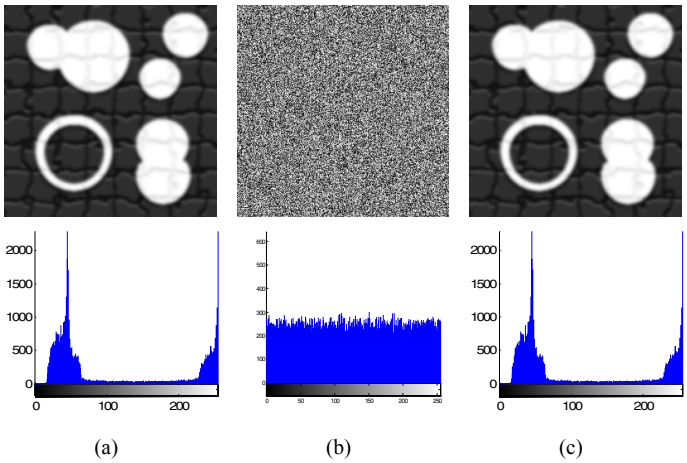
The pixel substitution changes the image histogram into uniform-like distribution.

IV. SIMULATION AND ANALYSIS

A. Simulation results

The encryption and decryption algorithms are implemented in MATLAB. The simulation results demonstrate that the proposed new algorithm shows good performances in image encryption.

The encrypted image in Figure 4(b) is completely different from the original image and cannot be recognized. This shows the success of the encryption algorithm. The decrypted image in Figure 4(c), getting from the decryption process, is the same as the original image in Figure 4(a). This shows the success of the decryption algorithm.



(a) (b) (c)

Figure 4. Simulation results of the proposed encryption algorithm: (a) the original image and its histogram; (b) the encrypted image and its histogram; (c) the decrypted image and its histogram

Histogram analysis is an important section to evaluate the property of the image encryption algorithms. We also observe the histograms of the original, encrypted and decrypted images. Histogram of the encrypted image has been equalized after the encryption process.

B. Security analysis

According to cryptographic requirements, a good encryption system should have a high level of security to resist many well-known attacks. Following the principle in [12], the security level of an encryption system depends on its security keys. If the key space is small or the key is not well-designed, the encryption system is not able to resist the different attacks, even though the encryption algorithm is much complicated. Here, the security key analysis is performed to test the security level of the proposed image encryption algorithm. To evaluate the performance of the proposed encryption system, information entropy is utilized for analysis.

1) Key space

One of the requirements for the security key is that the key space should be large enough to resist the brute-force attack. Given today's computer speed, the system has a certain level of security only if the key space is of size $k > 2^{100}$ [13]. The proposed encryption algorithm is a 240-bit encryption scheme with the key space size of $2^{240} \approx 1.7668 * 10^{72}$. Compared with the space requirement (2^{100}), the key space of this proposed encryption algorithm is more than twice large. It means that the algorithm is enough to withstand the brute-force attack.

2) Key sensitivity

A large key space does not mean using more bits to represent the same parameters and initial values. If you expand the space by doing so, the system will generate the same results with a similar key. Hence, another key requirement is that the encryption algorithm should be sensitive to the encryption key. The encryption key in the proposed encryption algorithm is composed of ten parts which determine the parameters and initial values. Every part consists of 24 bits which means that a single difference in the key will result in a value change (at least $5.9605 * 10^{-8}$). A well-known test has been performed in this paper. The original image is encrypted with the key1 and key2 to obtain two encrypted images. The absolute value of the difference between these two encrypted images is then obtained.

Key1="0123456789abcdefedcba98765432101234567 89abcdefedcba987654321"

Key2="0123456789abcdefedcba98765432101234567 89abcdefedcba987654320"

The difference between key1 and key2 is value of the last bit. It is easy to calculate that the encrypted image by key1 has 99.62% difference from the encrypted image by key2 in terms of pixel grey-scale values in Figure 5. From the difference image, it can be confirmed that a tiny change of the encryption key will result in a huge difference.

The key sensitivity analysis should also be tested in the decryption process. As shown in Figure 6, the same test performed in the decryption process using two different decryption keys (denoted as Dekey1 and Dekey2). Dekey1 is generated by the encryption process with the encryption key. Dekey2 is generated by making a slight change in the value of the first bit in Dekey1.

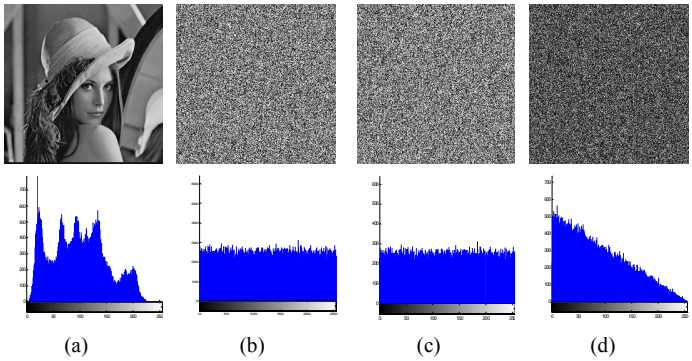
Dekey1="1861786789abcdefedcba98765432101234567 89abcdefedcba987654321"

Dekey2="9861786789abcdefedcba98765432101234567 89abcdefedcba987654321"

From the results shown in Figure 6, a slight change in the decryption key will lead to the failure of the image decryption. As shown in Figure 6(d), the decrypted image using dekey2 has not been recognized and its histogram is different from histogram of the original image. Therefore, only using the correct decryption key, the encrypted image can return to the original one with the same histogram as shown in Figure 6(c).

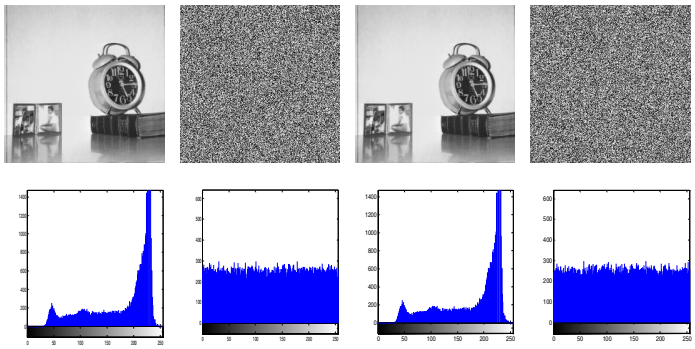
3) Information entropy

Histogram analysis just shows the result of the encryption algorithm in a qualitative way. To get the quantitative analysis, information entropy is utilized. Information entropy, as a measure of disorder, can quantify the uniformity of histogram. The function of the information entropr is defined as Eqn. (16).



(a) (b) (c) (d)

Figure 5. Key sensitivity test on the encryption keys: (a) original image and its histogram; (b) encrypted image (P1) using key1 and its histogram; (c) the encrypted image (P2) using key2 and its histogram;(d) difference image (|P1-P2|) and its histogram



(a) (b) (c) (d)

Figure 6. Key sensitivity test on the decryption keys: (a) original image and its histogram; (b) encrypted image and its histogram; (c) decrypted image using dekey1 and its histogram; (d) decrypted image using dekey2 and its histogram

$$H(I) = \sum_{i=0}^{F-1} P(i) \log_2 \frac{1}{P(i)} \qquad (16)$$

Here, P(i) represents the probability of pixels with the value equal to i (from 0 to F-1).

TABLE II. INFORMATION ENTROPY ANALYSIS

File name	Information entropy of original image	Information entropy of encrypted image
Lena image	7.5534	7.9669
Circle image	6.0408	7.9652
Clock image	6.7057	7.9667

In these tests on the grayscale images, F is equal to 8 and 8 bits are used to represent the pixel value. From Table II, information entropy has been increased with the encryption system and the information entropy of the encrypted image is almost near to 8. This confirms that the pixel values after encryption process seems random, which is sufficient secure for information leakage.

V. CONCLUSION

In this paper, a new chaotic system using a combination of three conventional one-dimensional chaotic maps has been proposed. The new system chooses the Sine map or the Tent map to generate the chaotic sequence according to the output value of the Logistic map. The system shows better chaotic performance by inheriting the high sensitivity to the initial conditions and expanding the range of parameters. At the same time, this combination makes the generation of the chaotic sequences more complicated and difficult to be identified by iterates and auto-correlation functions.

We have introduced a novel image encryption algorithm using the proposed new chaotic system. The SPN structure of the encryption algorithm ensures its properties of diffusion and confusion. Meantime, histogram analysis shows the encryption performance of the proposed algorithm. The security key analysis shows that algorithm has the sufficiently large key space to resist the brute-force attack and high sensitivity to the key changes for encryption and decryption. All these show that the proposed encryption algorithm has a high level of security.

VI. ACKNOWLEDGEMENT

This work was supported by Research Committee of the University of Macau under grant SRG007-FST12-ZYC and conference grant as well as the National Natural Science Foundation of China with Grant No. 61172089.

REFERENCES

[1] S. Lian, Y. Mao, and Z. Wang, "3D Extensions of Some 2D Chaotic Maps and Their Usage in Data Encryption," in *Control and Automation, 2003. ICCA '03. Proceedings. 4th International Conference on*, 2003, pp. 819-823.

[2] R. Matthews, "On the derivation of a Chaotic encryption algorithm," *Cryptologia,* vol. 8, pp. 29-41, 1984.

[3] N. Singh and A. Sinha, "Optical image encryption using Hartley transform and logistic map," *Optics Communications,* vol. 282, pp. 1104-1109, 2009.

[4] X. Yi, "Hash function based on chaotic tent maps," *IEEE Transactions on Circuits and Systems II: Express Briefs,* vol. 52, pp. 354-357, 2005.

[5] W. Yue, J. P. Noonan, and S. Agaian, "A wheel-switch chaotic system for image encryption," in *System Science and Engineering (ICSSE), 2011 International Conference on*, 2011, pp. 23-27.

[6] S. C. Phatak and S. S. Rao, "Logistic map: A possible random-number generator," *Physical Review E,* vol. 51, p. 3670, 1995.

[7] M. I. Sobhy and A. E. R. Shehata, "Methods of attacking chaotic encryption and countermeasures," in *Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference on*, 2001, pp. 1001-1004 vol.2.

[8] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing,* vol. 24, pp. 926-934, 2006.

[9] C. Fu, B.-b. Lin, Y.-s. Miao, X. Liu, and J.-j. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications,* vol. 284, pp. 5415-5423, 2011.

[10] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," *Optics Communications,* vol. 284, pp. 5290-5298, 2011.

[11] D. R.Stinson, *Cryptography.Theory and Practice.Third edition*: Chapman & Hall/CRC, 2006.

[12] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. New York: CRC Press, Inc., 1997.

[13] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos,* vol. 16, pp. 2129-2151, 2006.